

[Sign in](#)[Google](#)[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)[Advanced Search Preferences](#)

The "AND" operator is unnecessary -- we include all search terms by default. [[details](#)]

Web

Results 1 - 10 of about 887,000 for **copy protection and portable device and encryption**. (0.26 seconds)

FairPlay - Wikipedia, the free encyclopedia

The **encryption-free AAC files** will be offered on Apple's iTunes Store. ... of being locked into a specific **portable device** when they buy digital music. ... en.wikipedia.org/wiki/FairPlay - 40k - [Cached](#) - [Similar pages](#)

Digital rights management - Wikipedia, the free encyclopedia

The term is often confused with **copy protection** and **technical protection** ... who wish to use the music on their **portable device** an additional \$5 per month. ... en.wikipedia.org/wiki/Digital_Rights_Management - 82k - Apr 28, 2007 - [Cached](#) - [Similar pages](#)
[[More results from en.wikipedia.org](#)]

NewsFactor Network | Microsoft Debuts CD Copy-Protection Software

Consumers complained that such CDs were unplayable in CD-ROM drives, car stereos and **portable devices**. Additionally, users said **copy protection** prevented ...

www.newsfactor.com/perl/story/20509.html - [Similar pages](#)

[PDF] Copy Protection / DRM

File Format: PDF/Adobe Acrobat - [View as HTML](#)
Watermark as **protected**. • Enforcement: Playback / **Copy Devices** ... Content protection. – Creation: CSS **encryption**, Macrovision, CGMS flag, CPPM DVD-Audio ...
manifest-tech.com/docs/dixon_copy_drm_0611.pdf - [Similar pages](#)

A Cost Analysis of Windows Vista Content Protection

As part of the **bus-protection** scheme, **devices** are required to implement AES-128 **encryption** in order to receive content from Vista. ...
www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.txt - 170k - [Cached](#) - [Similar pages](#)

EETimes.com - Copy protection proposed for digital displays

The High-bandwidth Digital **Copy Protection** (HDCP) approach encrypts each pixel as it moves from a ... LDO extends battery run-time in **portable devices** ...
www.eetimes.com/story/OEG20000217S0039 - 48k - [Cached](#) - [Similar pages](#)

New DVDs spark copy-protection confusion - News - Video Software

Part of the problem is that the **copy protection** technology for the discs hasn't ... While the Apple iPod isn't the first **portable device** to support digital ...
www.cnet.com.au/software/video/0,239035364,240060381,00.htm - 82k - [Cached](#) - [Similar pages](#)

Copy protection control system - Patent 6591365

The player is shown as a **portable device** 40 with some form of removable ... The music is not **copy-protected**, and it is passed to the player as shown by ...
www.freepatentsonline.com/6591365.html - 50k - [Cached](#) - [Similar pages](#)

[PDF] A Copy Protection System for Digital Home Networks

File Format: PDF/Adobe Acrobat - [View as HTML](#)
SmartRight's end-to-end **encryption** system may coexist and interoperate with all currently available **copy protection** systems: inbound and outbound rules are ...
www.smartright.org/images/SMR/content/SmartRight_leaflet_white_jan03.pdf - [Similar pages](#)

EFF: Digital Rights Management and Copy Protection Schemes

As everyone knows, the AACs **encryption** scheme that restricts Blu-ray and HD DVD ... or DR^M (aka content or **copy protection**), to lock up your digital media. ...
www.eff.org/IP/DRM/ - 14k - [Cached](#) - [Similar pages](#)

[Sign in](#)[Google](#)[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)[Advanced Search Preferences](#)

The "AND" operator is unnecessary -- we include all search terms by default. [\[details\]](#)

Web Results 11 - 20 of about 888,000 for **copy protection and portable device and encryption**. (0.10 seconds)**[IEEE Spectrum: Loser: DVD Copy Protection, Take 2](#)**

It would stay encrypted when transferred to other devices and would be decrypted by ... The CSS encryption in the first generation of DVDs, which Johansen ...
www.spectrum.ieee.org/print/2703 - [Similar pages](#)

[IEEE Spectrum: Loser: DVD Copy Protection, Take 2](#)

It would stay encrypted when transferred to other devices and would be ... included when the first version of the **copy protection** specification is released. ...
www.spectrum.ieee.org/jan05/2703 - [Similar pages](#)

[EETimes.com - Content protection plan targets wireless home networks](#)

And while DTCP requires re-encryption at every digital device border, ... Micronas and co-chairman for the **copy protection** technology group of Europe-based ...
www.eetimes.com/story/OEG20020111S0060 - 52k - [Cached](#) - [Similar pages](#)

[\[PPT\] Cluster Copy Protection](#)

File Format: Microsoft Powerpoint - [View as HTML](#)
Broadcast Encryption Basics. Device keys. Each device is assigned a unique ...
"DVB-CPT Call for Proposals for Content Protection & Copy Management" ...
www.cptwg.org/Assets/Presentations/CPTWG%20-%20xCP-07-02.ppt -
[Similar pages](#)

[DMCA and the politics of copy protection@Everything2.com](#)

The **copy protection** policies of newer audio and video recording devices are ...
Even though the DMCA appears to make exceptions for fair use, **encryption** ...
everything2.com/index.pl?node_id=952746 - 38k - [Cached](#) - [Similar pages](#)

[\[PDF\] DVD Copy Protection: Take 2 - Spectrum, IEEE](#)

File Format: PDF/Adobe Acrobat
copy protection scheme designed to keep future gener- ... the various devices they own, including video servers and **portable** video ...
ieeexplore.ieee.org/iel5/6/30076/01377873.pdf - [Similar pages](#)

[Techdirt: The Copy Protection Myth](#)

Which is the point of this article, **copy protection** doesn't keep anything ... copying them to **portable devices**. The problem: the CSS **encryption** on the DVDs. ...
www.techdirt.com/articles/20050808/0233242.shtml - 43k - [Cached](#) - [Similar pages](#)

[Techdirt: The Copy Protection Myth](#)

It's not hard to see why **copy protection** on legally purchased CDs ... and copying them to **portable devices**. The problem: the CSS **encryption** on the DVDs. ...
www.techdirt.com/article.php?sid=20050808/0233242 - 43k - [Cached](#) - [Similar pages](#)
[More results from www.techdirt.com]

[Hetz Dongle: Software protection devices, copy protection ...](#)

software protection devices, copy protection, license management and **encryption** ... Works on the Com1 or Com2 port of any PC or Portable or notebook.
...

www.geocities.com/siliconvalley/vista/5429/dongle.html - 8k - [Cached](#) - [Similar pages](#)

[Registering copy protected material in a check-out, check-in ...](#)

In a limited-**copy protection** scheme, a check-out/check-in system is configured ... cards to record content material for playback on small **portable devices**. ...
www.freepatentsonline.com/7134145.html - 37k - [Cached](#) - [Similar pages](#)

[Sign in](#)[Google](#)[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)[Advanced Search](#)
[Preferences](#)

The "AND" operator is unnecessary -- we include all search terms by default. [\[details\]](#)

Web Results 21 - 30 of about 888,000 for **copy protection and portable device and encryption**. (0.37 seconds)

Breaking Barriers to Popularize Internet Streaming Broadcast

The current **copy-protection** scheme imposed on the consumer-type devices, however, ... [12] SDMI Portable Device - Part 1, Version 1.0 (Document Number ...
www.isoc.org/inet2000/cdproceedings/8g/8g_1.htm - 38k - [Cached](#) - [Similar pages](#)

[PDF] [14534 Macrovision \(e\)](#)

File Format: PDF/Adobe Acrobat

to **portable devices** that support Windows. Media. The labels also want **copy-protected** discs. to support CD burning, but only if it can be ...

www.macrovision.com/pdfs/macrovision-latimes.pdf - [Similar pages](#)

BDA Details Blu-Ray Disc Content Protection Technology

The technology also supports the managed **copy** feature, which enables authorized movement of content onto home network and **portable devices** ...
www.cdrinfo.com/Sections/News/Details.aspx?NewsId=17598 - 122k - Apr 29, 2007
- [Cached](#) - [Similar pages](#)

Oem. Optical Experts Manufacturing in Charlotte, NC

Data **encryption** is a key weapon to fighting content piracy. ... HexaLock is a solution for developers who want to create **copy protected** CD-ROMs and CD-R ...
www.oemdisc.com/services/copy.html - 16k - [Cached](#) - [Similar pages](#)

SDMI-Internet Players To Miss Holiday Season - Technology News by ...

Although the group did produce a first version of a **portable-device** ... With record companies free to choose whatever **copy protection** system they like, ...
www.techweb.com/wire/story/TWB19990923S0027 - 36k - [Cached](#) - [Similar pages](#)

CD Crack: Magic Marker Indeed -

The effect is that the **copy-protected** disc will play on standard CD players but not on computer CD-Rom drives, some **portable devices** and even some car ...
www.wired.com/science/discoveries/news/2002/05/52665 - 37k - Apr 28, 2007 -
Cached - [Similar pages](#)

HD DVD and Blu-ray delayed by AACS anti-copy standard - Engadget

In the days of analog, it was different; just release a device that ignored the **protection**. With 128 digital **encryption**, it's a whole new story. ...
www.engadget.com/2006/02/15/hd-dvd-and-blu-ray-delayed-by-aacs-anti-copy-standard/ - 95k - [Cached](#) - [Similar pages](#)

Freedom to Tinker » Blog Archive » CD Copy Protection: The Road to ...

Having set off down the road of CD **copy protection**, the music industry ... know you have it until you cannot **copy** your music onto your **portable device** ...
www.freedom-to-tinker.com/?p=939 - 145k - [Cached](#) - [Similar pages](#)

Slashdot | Longhorn's Copy Protection Standard

Longhorn's **Copy Protection** Standard -- article related to Microsoft, Windows, and Music. ... Re:**Encryption Circumvention Devices?** by That's Unpossible! ...
slashdot.org/articles/04/09/16/175211.shtml?id=201&tid=109&tid=141 - 223k -
Cached - [Similar pages](#)

Standardization activities

CEMA's Working Group 2 of sub-committee R4.8 works on **copy protection** ...
Interoperability means that an application on a HAVI device can detect and use the ...
www.chiariglione.org/leonardo/standards/opima/morristown/initiatives.html - 25k -
Cached - [Similar pages](#)

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)



PORTAL

USPTO

Search: The ACM Digital Library The Guide



Terms used copy protection and portable and encryption Found 48,845 of 200,192

Sort results by

relevance

Save results to a Binder

Try an Advanced Search

Display results

expanded form

Search Tips

Try this search in The ACM Guide

Open results in a new window

Results 1 - 20 of 200

Result page: **1** [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale

- 1 Software protection: Attacks and risk analysis for hardware supported software copy protection systems**



Weidong Shi, Hsien-Hsin S. Lee, Chenghuai Lu, Tao Zhang

October 2004 **Proceedings of the 4th ACM workshop on Digital rights management DRM '04**

Publisher: ACM Press

Full text available: [pdf\(167.21 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

<i>Recently, there is a growing interest in the research community to use tamper-resistant processors for software copy protection. Many of these tamper-resistant systems rely on a specially tailored secure processor to prevent, 1) illegal software duplication, 2) unauthorized software modification, and 3) unauthorized software reverse engineering. The published techniques primarily focused on feasibility demonstration and design details rather than analyzing security risks and potential a ...

Keywords: attack, copy protection, tamper resistance

- 2 Digital multimedia book: From digital audiobook to secure digital multimedia-book**



Lavinia Egidi, Marco Furini

July 2006 **Computers in Entertainment (CIE), Volume 4 Issue 3**

Publisher: ACM Press

Full text available: [pdf\(364.18 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Portable devices and wireless connections are creating a new scenario in which digital information is entering our lives in a massive way. In this article we consider MP3 audiobook applications and propose an approach to completely restyle the applications to the current mobile and multimedia scenario. Our mechanism introduces multimedia contents (images and text) into the audiobook application and synchronizes them with the MP3 audio stream. Multimedia contents are protected by a security syste ...

Keywords: multimedia applications, multimedia communications, multimedia over wireless, music distribution

- 3 Physical privacy: Privacy management for portable recording devices**



J. Alex Halderman, Brent Waters, Edward W. Felten

October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society WPES '04**

Publisher: ACM Press

Full text available: [pdf\(321.69 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The growing popularity of inexpensive, portable recording devices, such as cellular phone cameras and compact digital audio recorders, presents a significant new threat to privacy. We propose a set of technologies that can be integrated into recording devices to provide stronger, more accurately targeted privacy protections than other legal and technical measures now under consideration. Our design is based on an informed consent principle,

which it supports by the use of novel devices and pr ...

Keywords: camera phones, privacy, recording devices

- 4 **Key management and key exchange: A temporal key management scheme for secure broadcasting of XML documents**



Elisa Bertino, Barbara Carminati, Elena Ferrari
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**

Publisher: ACM Press

Full text available: pdf(242.89 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Secure broadcasting of web documents is becoming a crucial need for many web-based applications. Under the broadcast document dissemination strategy a web document source periodically broad-casts (portions of) its documents to a possibly large community of subjects, without the need of explicit subject requests. By secure broadcasting we mean that the delivery of information to subjects must obey the access control policies of the document source. Since different subjects may have the right to ...

Keywords: XML, secure broadcasting, temporal key management

- 5 **Innovation, management & strategy: Towards a framework for understanding the effectiveness of digital content exploitation strategies**



Ernst-Jan Goedvolk, Edward Faber, René W. Wagenaar
March 2004 **Proceedings of the 6th international conference on Electronic commerce ICEC '04**

Publisher: ACM Press

Full text available: pdf(259.74 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Due to initiatives like Napster and Kazaa the business case for delivering protected digital content remains problematic. Still little is known about the effectiveness of content exploitation strategies. In this paper the literature on content protection, provisioning and usage is reviewed. Based on this review a causal framework is developed, which seeks to explain the effectiveness of content exploitation strategies. The paper ends with formulating a research agenda for studying content exploi ...

Keywords: content exploitation, content protection

- 6 **Limited-lifetime shared-access in mobile systems**

Zygmunt J. Haas, Sanjoy Paul

June 1995 **Wireless Networks**, Volume 1 Issue 2

Publisher: Kluwer Academic Publishers

Full text available: pdf(861.11 KB)

Additional Information: [full citation](#), [abstract](#), [references](#)

In this paper, we propose a simple access protocol to shared information in a mobile environment. The objective of the proposed scheme is to allow a specified set of users access to shared information and protect the confidentiality of the information from users outside this set. The set of users may be updated from time to time. In particular, the duration during which a user is allowed access to the shared information may be restricted. Furthermore, the information itself has limited life ...

- 7 **Protecting VoD the easier way**



Carsten Griwodz, Oliver Merkel, Jana Dittmann, Ralf Steinmetz

September 1998 **Proceedings of the sixth ACM international conference on Multimedia MULTIMEDIA '98**

Publisher: ACM Press

Full text available: pdf(897.94 KB)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

Keywords: copyright protection, corruption, multimedia, video-on-demand

- 8 **Future of intellectual property: How copyright became controversial**



Drew Clark

April 2002

Proceedings of the 12th annual conference on Computers, freedom and privacy CFP '02

Publisher: ACM Press

Full text available: [pdf\(52.48 KB\)](#)Additional Information: [full citation](#), [abstract](#), [index terms](#)

How did copyright become controversial? In a phrase, the Digital Millennium Copyright Act (DMCA). Although many of legal controversies that have swirled since its October 1998 passage trace their roots to other elements of copyright law, the DMCA created a new feature in copyright law that has crystallized why so many academics, librarians, computer users, and technology entrepreneurs object to what they regard as the overreaching nature of copyright law.

This signal feature ...

9 DRM experience: Digital rights management in a 3G mobile phone and beyond

Thomas S. Messerges, Ezzat A. Dabbish

October 2003 Proceedings of the 3rd ACM workshop on Digital rights management DRM '03

Publisher: ACM Press

Full text available: [pdf\(306.59 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

In this paper we examine how copyright protection of digital items can be securely managed in a 3G mobile phone and other devices. First, the basic concepts, strategies, and requirements for digital rights management are reviewed. Next, a framework for protecting digital content in the embedded environment of a mobile phone is proposed and the elements in this system are defined. The means to enforce security in this system are described and a novel "Family Domain" approach to content management ...

Keywords: MPEG-21, copyright protection, cryptography, digital content, digital rights management, embedded system, key management, mobile phone, open mobile alliance, security

10 Processor microarchitecture II: AEGIS: architecture for tamper-evident and tamper-resistant processing

G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas Devadas

June 2003 Proceedings of the 17th annual international conference on Supercomputing ICS '03

Publisher: ACM Press

Full text available: [pdf\(286.90 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We describe the architecture for a single-chip aegis processor which can be used to build computing systems secure against both physical and software attacks. Our architecture assumes that all components external to the processor, such as memory, are untrusted. We show two different implementations. In the first case, the core functionality of the operating system is trusted and implemented in a security kernel. We also describe a variant implementation assuming an untrusted operating s ...

Keywords: certified execution, secure processors, software licensing

11 Practice: Some security alternatives for encrypting information on storage devices

Robin Snyder

September 2006 Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD '06

Publisher: ACM Press

Full text available: [pdf\(63.12 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Almost every few weeks there is some breaking news about some organization that has lost information via the physical loss of an unencrypted storage device. This paper reviews some alternatives for encrypting information on storage devices and how those alternatives might be used. The open source TrueCrypt system is covered is some detail. Some suggestions for information security policy guidelines are provided. From personal data to enterprise data, information security is becoming increasin ...

Keywords: encrypting file systems, storage devices

12 Protocol failure in the escrowed encryption standard

Matt Blaze

November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security CCS '94**

Publisher: ACM Press

Full text available: pdf(953.18 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The Escrowed Encryption Standard (EES) defines a US Government family of cryptographic processors, popularly known as "Clipper" chips, intended to protect unclassified government and private-sector communications and data. A basic feature of key setup between pairs of EES processors involves the exchange of a "Law Enforcement Access Field" (LEAF) that contains an encrypted copy of the current session key. The LEAF is intended to facilitate government access to the cl ...

13 Security: SECA: security-enhanced communication architecture

Joel Coburn, Srivaths Ravi, Anand Raghunathan, Srimat Chakradhar

September 2005 **Proceedings of the 2005 international conference on Compilers, architectures and synthesis for embedded systems CASES '05**

Publisher: ACM Press

Full text available: pdf(390.53 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

In this work, we propose and investigate the idea of enhancing a System-on-Chip (SoC) communication architecture (the fabric that integrates system components and carries the communication traffic between them) to facilitate higher security. We observe that a wide range of common security attacks are manifested as abnormalities in the system-level communication traffic. Therefore, the communication architecture, with its global system-level visibility, can be used to detect them. The communicati ...

Keywords: AMBA Bus, access control, architecture, attacks, bus, communication, digital rights management (DRM), intrusion detection, security, security-aware design, small embedded systems, system-on-chip (SoC)

14 Surfing the net for software engineering notes: Surfing the net for software engineering notes

Mark Doernhoefer

November 2006 **ACM SIGSOFT Software Engineering Notes**, Volume 31 Issue 6

Publisher: ACM Press

Full text available: pdf(786.88 KB)

Additional Information: [full citation](#), [abstract](#)

I talk about software security on a regular basis in this column. Past articles have featured web sites addressing security design tips and techniques, security reporting sites, and other security resources available on the Internet. I'd like to stop talking about security but the subject seems to keep coming up in the press. Recent news reports on lost laptops compromising personal data, security of voting machines, new zero day exploits, and new rootkits would indicate that we are still not wh ...

15 Cryptography and data security

Dorothy Elizabeth Robling Denning

January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(19.47 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)**From the Preface (See Front Matter for full Preface)**

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

16 Student papers: Securing varieties of file systems

Philippa Fendler



October 2004 Proceedings of the 1st annual conference on Information security curriculum development InfoSecCD '04

Publisher: ACM Press

Full text available: [pdf\(69.32 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

In this paper, I describe the different ways to security different storage media. Important is not just the security of data in frequent use, but also data that is no longer needed. Regardless of media or system, information security should always be applied in layers so that any one system won't be compromised when falling into the wrong hands.

Keywords: NTTS, data destruction, disks, encryption, fat, memory cards, mobile media, optical media, securing reactively and proactively, security

17 Secure and selective dissemination of XML documents



Elisa Bertino, Elena Ferrari

August 2002 **ACM Transactions on Information and System Security (TISSEC)**, Volume 5

Issue 3

Publisher: ACM Press

Full text available: [pdf\(678.34 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

XML (eXtensible Markup Language) has emerged as a prevalent standard for document representation and exchange on the Web. It is often the case that XML documents contain information of different sensitivity degrees that must be selectively shared by (possibly large) user communities. There is thus the need for models and mechanisms enabling the specification and enforcement of access control policies for XML documents. Mechanisms are also required enabling a secure and selective dissemina ...

Keywords: Access control, XML, secure distribution

18 Hardware protection against software piracy



Tim Maude, Derwent Maude

September 1984 **Communications of the ACM**, Volume 27 Issue 9

Publisher: ACM Press

Full text available: [pdf\(843.02 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

A system that prevents illicit duplication of proprietary software is suggested. It entails the customization of the programs for each computer by encryption. The use of a public key cryptogram for this purpose means that anyone can customize programs, but neither other programmers nor the people having complete access to the target computer can obtain copies that will run on other machines. A possible implementation of the system is considered in some detail. It is based on a hardware secu ...

Keywords: proprietary software protection, public key cryptography, software encryption, software piracy

19 A functional taxonomy for software watermarking

Jasvir Nagra, Clark Thomborson, Christian Collberg

January 2002 **Australian Computer Science Communications , Proceedings of the twenty-fifth Australasian conference on Computer science - Volume 4 ACSC '02**, Volume 24 Issue 1

Publisher: Australian Computer Society, Inc., IEEE Computer Society Press

Full text available: [pdf\(1.19 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Despite the recent surge of interest in digital watermarking technology from the research community, we lack a comprehensive and precise terminology for software watermarking. In this paper, we attempt to fill that gap by giving distinctive names for the various protective functions served by software watermarks: Validation Mark, Licensing Mark, Authorship Mark and Fingerprinting Mark. We identify the desirable properties and specific vulnerabilities of each type of watermark, and we illustrate ...

Keywords: authentication, fingerprint, software authorship, software licensing, steganography, watermark

20 Systems: Securing sensitive content in a view-only file system



Kevin Borders, Xin Zhao, Atul Prakash
October 2006 **Proceedings of the ACM workshop on Digital rights management DRM '06**

Publisher: ACM Press

Full text available: [pdf\(357.44 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

One of the most fundamental problems in computer security is protecting sensitive digital information from unauthorized disclosure. There are a number of challenges, such as spyware, removable media, and mobile devices, which make this a very hard problem. The problem becomes even more difficult when the adversary is somebody who is authorized to view the data. This is what is commonly referred to as an insider information leak. Insider leaks often occur out of malice, but sometimes are just due ...

Keywords: digital rights management, file systems, information leakage, insider abuse, virtual machines

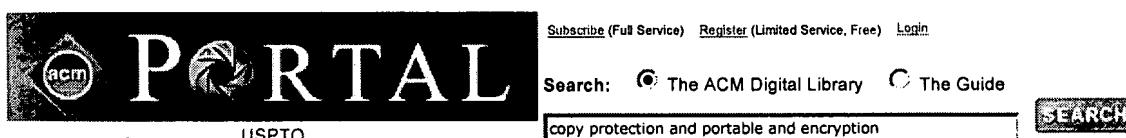
Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)



THE ACM DIGITAL LIBRARY

Terms used copy protection and portable and encryption

Found 48,845 of 200,192

Sort results by

relevance

Save results to a Binder

Try an Advanced Search

Display results

expanded form

Search Tips

Try this search in The ACM Guide

Open results in a new window

Results 21 - 40 of 200

Result page: previous

1 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

21 Copy detection for intellectual property protection of VLSI designs

Andrew B. Kahng, Darko Kirovski, Stefanus Mantik, Miodrag Potkonjak, Jennifer L. Wong
November 1999 **Proceedings of the 1999 IEEE/ACM international conference on Computer-aided design ICCAD '99**

Publisher: IEEE Press

Full text available: pdf(109.67 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We give the first study of copy detection techniques for VLSI CAD applications; these techniques are complementary to previous watermarking-based IP protection methods in finding and proving improper use of design IP. After reviewing related literature (notably in the text processing domain), we propose a generic methodology for copy detection based on determining basic elements within structural representations of solutions (IPs), calculating (context-independent) signature ...

22 Peer-to-peer data trading to preserve information



Brian F. Cooper, Hector Garcia-Molina

April 2002 **ACM Transactions on Information Systems (TOIS)**, Volume 20 Issue 2

Publisher: ACM Press

Full text available: pdf(490.65 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Data archiving systems rely on replication to preserve information. This paper discusses how a network of autonomous archiving sites can trade data to achieve the most reliable replication. A series of binary trades among sites produces a peer-to-peer archiving network. Two trading algorithms are examined, one based on trading collections (even if they are different sizes) and another based on trading equal sized blocks of space (which can then store collections). The concept of *deeds* is ...

Keywords: Data replication, digital archiving, digital library, fault tolerance, resource negotiation

23 Encryption and Secure Computer Networks



Gerald J. Popek, Charles S. Kline

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

Publisher: ACM Press

Full text available: pdf(2.50 MB)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

24 Code optimization II: Hiding program slices for software security

Xiangyu Zhang, Rajiv Gupta

March 2003 **Proceedings of the international symposium on Code generation and optimization: feedback-directed and runtime optimization CGO '03**

Publisher: IEEE Computer Society

Full text available: pdf(1.05 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Given the high cost of producing software, development of technology for prevention of

software piracy is important for the software industry. In this paper we present a novel approach for preventing the creation of unauthorized copies of software. Our approach splits software modules into *open* and *hidden* components. The open components are installed (executed) on an unsecure machine while the hidden components are installed (executed) on a secure machine. We assume that while open ...

25 Protecting applications with transient authentication



Mark D. Corner, Brian D. Noble

May 2003

Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03

Publisher: ACM Press

Full text available: [pdf\(294.40 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...

26 DRM usability and legal issues: Import/export in digital rights management



Reihaneh Safavi-Naini, Nicholas Paul Sheppard, Takeyuki Uehara

October 2004

Proceedings of the 4th ACM workshop on Digital rights management DRM '04

Publisher: ACM Press

Full text available: [pdf\(211.60 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The inherently controlled nature of digital rights management systems does little to promote inter-operability of systems provided by different vendors. In this paper, we consider import and export functionality by which multimedia protected by one digital rights management regime can be made available to a multimedia device that supports a different digital rights management regime, without compromising the protection afforded to the content under the original regime. We first identify speci ...

Keywords: digital rights management, export, import, inter-operability

27 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design



Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan

June 2004

Proceedings of the 41st annual conference on Design automation DAC '04

Publisher: ACM Press

Full text available: [pdf\(209.10 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is ...*

Keywords: PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses

28 Verifiable distributed oblivious transfer and mobile agent security



Sheng Zhong, Yang Richard Yang

September 2003

Proceedings of the 2003 joint workshop on Foundations of mobile computing DIALM-POMC '03

Publisher: ACM Press

Full text available: [pdf\(344.93 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The mobile agent is a fundamental building block of the mobile computing paradigm. In mobile agent security, oblivious transfer (OT) from a trusted party can be used to protect the agent's privacy and the hosts' privacy. In this paper, we introduce a new cryptographic primitive called *Verifiable Distributed Oblivious Transfer (VDOT)*, which

allows us to replace a single trusted party with a group of threshold trusted servers. The design of VDOT uses two novel techniques, *consistency ver* ...

Keywords: oblivious transfer, resiliency to corruptions, secure mobile agents and mobile code, verifiable secret sharing

- 29 [Information protection methods: Display-only file server: a solution against information theft due to insider attack](#)



Yang Yu, Tzi-cker Chiueh

October 2004 **Proceedings of the 4th ACM workshop on Digital rights management DRM '04**

Publisher: ACM Press

Full text available: pdf(311.80 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Insider attack is one of the most serious cybersecurity threats to corporate America. Among all insider threats, information theft is considered the most damaging in terms of potential financial loss. Moreover, it is also especially difficult to detect and prevent, because in many cases the attacker has the proper authority to access the stolen information. According to the 2003 CSI/FBI Computer Crime and Security Survey, theft of proprietary information was the single largest category of los ...

Keywords: access, digital rights management, information theft, insider attack

- 30 [Applied cryptography: Attacking and repairing the winZip encryption scheme](#)



Tadayoshi Kohno

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**

Publisher: ACM Press

Full text available: pdf(171.91 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#), [review](#)

WinZip is a popular compression utility for Microsoft Windows computers, the latest version of which is advertised as having "easy-to-use AES encryption to protect your sensitive data." We exhibit several attacks against WinZip's new encryption method, dubbed "AE-2" or "Advanced Encryption, version two." We then discuss secure alternatives. Since at a high level the underlying WinZip encryption method appears secure (the core is exactly Encrypt-then-Authenticate using AES-CTR and HMAC-SHA1), ...

Keywords: WinZip, Zip, applied cryptography, attacks, compression, encryption, security fixes

- 31 [On incremental file system development](#)



Erez Zadok, Rakesh Iyer, Nikolai Joukov, Gopalan Sivathanu, Charles P. Wright

May 2006 **ACM Transactions on Storage (TOS)**, Volume 2 Issue 2

Publisher: ACM Press

Full text available: pdf(260.40 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Developing file systems from scratch is difficult and error prone. Using layered, or stackable, file systems is a powerful technique to incrementally extend the functionality of existing file systems on commodity OSes at runtime. In this article, we analyze the evolution of layering from historical models to what is found in four different present day commodity OSes: Solaris, FreeBSD, Linux, and Microsoft Windows. We classify layered file systems into five types based on their functionality and ...

Keywords: I/O manager, IRP, Layered file systems, VFS, extensibility, stackable file systems, vnode

- 32 [Implementing an untrusted operating system on trusted hardware](#)



David Lie, Chandramohan A. Thekkath, Mark Horowitz

October 2003 **ACM SIGOPS Operating Systems Review , Proceedings of the nineteenth ACM symposium on Operating systems principles SOSP '03**, Volume 37 Issue 5

Publisher: ACM Press

Full text available:

Additional Information:

 pdf(280.87 KB)[full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Recently, there has been considerable interest in providing "trusted computing platforms" using hardware----TCPA and Palladium being the most publicly visible examples. In this paper we discuss our experience with building such a platform using a traditional time-sharing operating system executing on XOM----a processor architecture that provides copy protection and tamper-resistance functions. In XOM, only the processor is trusted; main memory and the operating system are not trusted. Our opera ...

Keywords: XOM, XOMOS, untrusted operating systems

- 33 [Workshop on architectural support for security and anti-virus \(WASSA\): Towards the issues in architectural support for protection of software execution](#) 



Weidong Shi, Hsien-Hsin S. Lee, Chenghuai Lu, Mrinmoy Ghosh

March 2005 **ACM SIGARCH Computer Architecture News**, Volume 33 Issue 1

Publisher: ACM Press

Full text available:  pdf(438.30 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Recently, there is a growing interest in the research community to employ tamper-resistant processors for software protection. Many of these proposed systems rely on a specially tailored secure processor to prevent 1) illegal software duplication, 2) unauthorized software modification, and 3) unauthorized software reverse engineering. Most of these works primarily focus on the feasibility demonstration and design details rather than trying to elucidate many fundamental issues that are either "el ...

Keywords: attack, copy protection, encryption, security, tamper resistance

- 34 [Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm](#) 



Mihir Bellare, Tadayoshi Kohno, Chanathip Namprempre

May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2

Publisher: ACM Press

Full text available:  pdf(404.99 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#), [review](#)

The *secure shell* (SSH) protocol is one of the most popular cryptographic protocols on the Internet. Unfortunately, the current SSH authenticated encryption mechanism is insecure. In this paper, we propose several fixes to the SSH protocol and, using techniques from modern cryptography, we prove that our modified versions of SSH meet strong new chosen-ciphertext privacy and integrity requirements. Furthermore, our proposed fixes will require relatively little modification to the SSH protoc ...

Keywords: Authenticated encryption, secure shell, security proofs, stateful decryption

- 35 [Security: Secrecy, flagging, and paranoia: adoption criteria in encrypted email](#) 



Shirley Gaw, Edward W. Felten, Patricia Fernandez-Kelly

April 2006 **Proceedings of the SIGCHI conference on Human Factors in computing systems CHI '06**

Publisher: ACM Press

Full text available:  pdf(502.61 KB)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We consider the social context behind users' decisions about whether and when to encrypt email, interviewing a sample of users from an organization whose mission requires secrecy. Interview participants varied in their level of technical sophistication and in their involvement with secrets. We found that users saw universal, routine use of encryption as paranoid. Encryption flagged a message not only as confidential but also as urgent, so users found the encryption of mundane messages annoying. ...

Keywords: activism, encrypted e-mail, extended case method, security

- 36 [Intrusion detection and modeling: Augmenting storage with an intrusion response primitive to ensure the security of critical data](#) 



Ashish Gehani, Surendar Chandra, Gershon Kedem

March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**

Publisher: ACM Press

Full text available:  pdf(326.59 KB)

Additional Information: [full citation](#), [abstract](#), [references](#)

Hosts connected to the Internet continue to suffer attacks with high frequency. The use of an intrusion detector allows potential threats to be flagged. When an alarm is raised, preventive action can be taken. A primary goal of such action is to assure the security of the data stored in the system. If this operation is effected manually, the delay between the alarm and the response may be enough for an intruder to cause significant damage. The alternative proposed in this paper is to provide a re ...

37 A secure distributed capability based system (extended abstract)



Howard L. Johnson, John F. Koegel, Rhonda M. Koegel

October 1985 **Proceedings of the 1985 ACM annual conference on The range of computing : mid-80's perspective: mid-80's perspective ACM '85**

Publisher: ACM Press

Full text available:  pdf(1.22 MB)

Additional Information: [full citation](#), [references](#), [index terms](#)

Keywords: capability architecture, computer security, distributed system security, network encryption

38 Healthcare data integration and exchange: Bridging a gap in the proposed personal health record



Wai Gen Yee, Brett Trockman

November 2006 **Proceedings of the international workshop on Healthcare information and knowledge management HIKM '06**

Publisher: ACM Press

Full text available:  pdf(280.88 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The emerging electronic health record infrastructure is guiding records to be stored in repositories that collectively supply a patient's comprehensive health history. However, legal and technological constraints may keep such a system from delivering health histories in a timely manner (i.e., when medical attention is needed). To get around this, we propose a design for a portable personal health record system that complies with HIPAA standards of security and interaction. The authenticity of s ...

Keywords: HIPAA, personal health record, portability, security

39 On specifying security policies for web documents with an XML-based language



Elisa Bertino, Silvana Castano, Elena Ferrari

May 2001 **Proceedings of the sixth ACM symposium on Access control models and technologies SACMAT '01**

Publisher: ACM Press

Full text available:  pdf(290.20 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The rapid growth of the Web and the ease with which data can be accessed facilitate the distribution and sharing of information. Information dissemination often takes the form of documents that are made available at Web servers, or that are actively broadcasted by Web servers to interested clients. In this paper, we present an XML-compliant formalism for specifying security-related information for Web document protection. In particular, we introduceX-Sec, an XML-based lang ...

Keywords: XML, access control, security policies, subject credentials

40 A secure multicast protocol with copyright protection



Hao-hua Chu, Lintian Qiao, Klara Nahrstedt, Hua Wang, Ritesh Jain

April 2002 **ACM SIGCOMM Computer Communication Review**, Volume 32 Issue 2

Publisher: ACM Press

Full text available:  pdf(301.97 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We present a simple, efficient, and secure multicast protocol with copyright protection in an open and insecure network environment. There is a wide variety of multimedia

applications that can benefit from using our secure multicast protocol, e.g., the commercial pay-per-view video multicast, or highly secure military intelligence video conference. Our secure multicast protocol is designed to achieve the following goals. (1) It can run in any open network environment. It does not rely on any sec ...

Keywords: copyright protection, key distribution, multicast security, watermark

Results 21 - 40 of 200

Result page: [previous](#) [1](#) **2** [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)